



# ***MicroLatch***<sup>TM</sup>

## BIOCARD User Guide

# Contents

Chapter 1 - Overview	3
What's in the box	4
Before You Begin	4
Programming the Internal Proximity Tags	5
Chapter 2 - Getting Started	7
Chapter 3 - Standalone Mode	8
Setting up your BIOCARD for the first time	8
Normal operation of your BIOCARD	10
Enrolling additional User Fingers	10
Erase Administrator/Users	10
Chapter 4 - Corporate Mode	12
What you need	12
Installing the Microlatch BIOCARD Manager Application	13
Initialise a BIOCARD in Corporate Mode	13
Enrol Corporate User	14
Erase Corporate User	16
Chapter 5 - About the Battery	17
Charging the Battery	17
Chapter 6 - Warranty Information	18

# Chapter 1 - Overview

Thank you for purchasing a Microlatch™ BIOCARD™.

Microlatch™ BIOCARD™ takes biometric products and solutions to the next level of security and convenience. BIOCARD™ overcomes the biggest single problem with traditional 'Access', where if the 'Proximity Card' is lost, stolen or borrowed, a person other than the Proximity Card owner can then gain access to the area that the Proximity Card controls.

The BIOCARD™ confirms the identity of the user, whether gaining access to a physical building or a PC network. The implementation of BIOCARD is simple, issue to the user in the exact same manner as a traditional access card or 'proximity card'. The user enrols his fingerprints into the BIOCARD and it is ready for use. The existing access card readers will automatically accept the BIOCARD, exactly the same as any proximity card, therefore no change to existing infrastructure. There is an option for a dual card BIOCARD version, one 'non-secure' that operates all the time like any other proximity card and one 'secure', which will only transmit an access signal for a short period of time after successful fingerprint verification via the built-in biometric scanner.

The BIOCARD™ is able to be used on ALL existing proximity or smart contactless readers, providing easy integration into already operational security systems.

## What's in the box

- 10x BIOCARD devices
- 10x USB Cable (for recharge only)
- 1x User manual (can also be downloaded from [www.microlatch.com](http://www.microlatch.com))

## Before You Begin

Please make sure you take the time to read through this operation guide BEFORE you begin the installation and configuration of your BIOCARD™.



## Programming the Internal Proximity Tags

The factory default setting for the BIOACRD is UNSECURE, meaning pressing the button on the front of the device will activate the internal ‘secure’ proximity tag – does not require any fingerprint operation. This allows for the ‘secure’ proximity tag within the BIOCARD to be programmed with I/Ds before enrolment via Standalone Mode (*refer to chapter 3*) or Corporate Mode (*refer to chapter 4*).

To activate the ‘secure’ proximity tag before enrolment has occurred, simply press the button. The secure proximity tag will activate for a period of 30 seconds before being disabled. If installed, the second ‘non-secure’ proximity tag is the same as a normal proximity card; it has no user fingerprint verification requirement and operates constantly.

Please refer to the relevant Proximity Reader User guides for information on programming the internal proximity tags to work with your chosen proximity reader/s. The BIOCARD is programmed in exactly the same manner as ALL traditional proximity and smart access cards or credentials.

Proximity Tags available in BIOCARD; please refer to packaging information to see what type of tag is installed.

- HID Prox
- HID iClass
- NFC Credit or Debit Cards
- DesFire
- Mifare
- Indala
- Legic
- Sony
- Hitag
- EM
- Temic

## Chapter 2 - Getting Started

Before you can use your BIOCARD, you require to fully charge the battery (refer to chapter 5). Plug in the USB cable supplied with your BIOCARD to a USB port of a computer or any 5V USB power adaptor. This will take up to 3hrs. The area around the USB port will glow a green fade colour when fully charged.

Once your BIOCARD is fully charged you will need to decide what mode you would like it to operate in.

**NOTE:** When using the Corporate USB cable supplied with the PC BIOCARD Manager application software, the charging blue light and the fully charged green light are both solid, not fade. The solid light indication confirms the attachment of the Corporate USB cable.

The BIOCARD had two modes:

1. **Standalone Mode** (refer to chapter 3)  
*Individuals or small number of users*
2. **Corporate Mode** (refer to chapter 4)  
*Medium to large businesses*  
*\*Requires Corporate Mode Starter Kit sold separately.*

## Chapter 3 - Standalone Mode

The BIOCARD is shipped in 'Standalone Mode' by default. This means the device will be controlled by the first two fingers that are enrolled. These two fingers become the administrator fingers and have full control over the device much like the administrator of a computer.

The BIOCARD is able to enrol two types of users:

1. **User:** this is a person who once enrolled can use the device for access but has no administrator rights i.e. cannot add or delete other users.
2. **Administrators:** this is a person who has the normal permissions of a user with the ability to add and delete all users.

## Setting up your BIOCARD for the first time

1. Press the button on the front of the device.
2. A rotating Cyan (light blue) light will appear around the button showing the device has no fingers enrolled (default state) and is ready to enrol an 'administrator' finger.
3. Swipe your finger; the light indication will go blank for a second then start to rotate with a Cyan light again. Repeat the finger swipe processes until you are presented with a solid green glow around the

button (this could take up to approx. 10 swipes to get an accurate template of your fingerprint).

4. The device will then proceed directly into the enrolment process of a second '*administrator*' finger. This is a backup in the event that the first '*administrator*' finger is damaged by a cut etc. and is unable to be verified. Repeat steps 2 to 3.
5. After successful enrolment of the second '*administrator*' finger, the device then proceeds directly into enrolment of a '*user finger*'. This is shown by a rotating Magenta (purple) light around the button.
6. Swipe your new '*user*' finger; the light indication will go blank for a second then start to rotate with Magenta light again. Repeat the finger swipe process until you are presented with a solid green glow around the button (this takes approx. 10 swipes to get an accurate template of your fingerprint).
7. Repeat Step 6 until the desired number of '*user*' fingers are enrolled.
8. To exit the enrolment procedure, simply leave the device for 30 seconds and the unit will return to standby mode.

## Normal operation of your BIOCARD

To use your BIOCARD:

1. Press the button on the front of the device.
2. A rotating Blue light will appear around the button, showing the device is ready to check a fingerprint.
3. Swipe an already enrolled 'administrator' or 'user' finger.
4. Successful verification is shown by a solid green glow around the button; unsuccessful verification is shown by a solid red glow around the button.
5. The internal proximity tag will remain active for 30 seconds after a successful verification of a finger.

## Enrolling additional User Fingers

1. Press the button on the front of the device.
2. A rotating Blue light will appear around the button, showing the device is ready to check a fingerprint.
3. Swipe an already enrolled 'administrator' finger.
4. A solid green light around the button indicates a successful verification (red indicates unsuccessful verification).
5. Press and hold down the button immediately while still green until a rotating Magenta light appears around the button. This shows the device is ready to enrol a user fingerprint.
6. Swipe your new 'user' finger; the light indication will go blank for a second then start to rotate with a

Magenta colour again. Repeat the finger swipe process until you are presented with a green glow indication around the button (this takes approx. 10 swipes to get an accurate template of your fingerprint).

7. Repeat steps 6 and 7 until desired number of user fingers are enrolled. To exit the enrolment procedure, simply leave the device for 30 seconds and the unit will return to standby mode.

## **Erase Administrator/Users**

A factory reset is able to be performed on the device to erase ALL administrator/users. This will take the device back to its default factory settings.

NOTE: This can only be performed by an administrator and will ERASE ALL ENROLLED ADMINISTRATORS/USERS from the device.

1. Press the button on the front of the device.
2. A rotating Blue light will appear around the button, showing the device is ready to check a fingerprint.
3. Swipe an already enrolled 'administrator' finger.
4. A solid green light around the button indicates a successful verification (red indicates unsuccessful verification).
5. Press and hold down the button immediately while still green.

6. Continue to hold down button, ignoring all colour indications until a rotating Magenta light appears around the button.
7. Swipe an '*administrator*' finger (approx. 10 times as done when enrolling a finger)
8. A solid yellow glow will appear around the button, immediately press and hold down the button while still yellow.
9. A rotating cyan light indicates that all administrators/users have been erased and the device has been factory reset.
10. The device is now ready for enrolment for the first time (see *Setting up your BIOCARD for the first time*)

NOTE: Until a new '*administrator*' is enrolled the device is **UNSECURE**.

## Chapter 4 - Corporate Mode

*'Corporate Mode'* is to be used when medium to large scale business want to issue a BIOCARD to individual/s without giving the users the ability to enrol or erase themselves or others after the initial enrolment procedure. In effect *'Corporate Mode'* gives an organisation administrator control over their issued BIOCARDS. This allows a BIOCARD to be erased in the event the BIOCARD needs to be reissued to another user or the original user is no longer needed.

The enrolment and erasure process is done via the ***Microlatch BIOCARD Manager*** application. This application securely restricts a BIOCARD to a computer and/or company. Once a BIOCARD has been activated in corporate mode it can only be enrolled or erased from a ***Microlatch BIOCARD Manager*** application with access

### What you need

PC; running Microsoft Windows operating system.

In addition to the BIOCARD device you will need to purchase separately:

- Corporate Mode Starter Kit (*includes an installation CD & USB Serial Programming Cable*)

## Installing the Microlatch BIOCARD Manager Application

1. Insert installation CD supplied in the Corporate Mode Starter Kit. Follow the on screen instructions.
2. Open the Microlatch BIOCARD Manager application.
3. You will be prompted to enter a storage location for the database file. Use the Browse button to select a folder location. This can be on a local computer or on a server (security of the database is the responsibility of the organisation/individual). Click the '*Update*' button, if the folder location is new a message will appear stating that the database does not exist, click '*OK*' to create the database.
4. The Microlatch BIOCARD Manager application is now ready to use.

## Initialise a BIOCARD in Corporate Mode

1. Open the Microlatch BIOCARD Manager application.
2. Connect a BIOCARD to a USB port on your computer, using the USB Serial cable that came with your Corporate Mode Starter Kit.
3. Click the '*Query*' button; if the BIOCARD connected has not already been initialised as a Corporate Mode BIOCARD, a message stating '*Uninitialised*' will be displayed.

4. **READ POINT 5 below before proceeding to this step.** Click either the 'Erase' or 'Learn' button to assign the BIOCARD with a serial number; this serial number is also assigned in the database.
5. **IMPORTANT NOTE: Once the above operation is performed, the BIOCARD will only be able to be enrolled and erased by a BIOCARD Manager application with access to the same database it was or is being initialised with.**
6. A solid Green light will flash around the BIOCARD button when corporate mode initialisation has been successful.

## **BACKUP BIOCARD Manager Database**

**NOTE:** Once the BIOCARD is initialized in corporate mode, it is important to back-up or copy the database immediately. Once the database has been created from the initial 'Update' procedure and 'OK' was selected, this database folder will contain all the files and serial numbers of BIOCARD's initialized by the BIOCARD Manager software. The database folder and all files should be copied and stored securely. In addition, if more BIOCARD's are added to the database, a procedure for update copying should be followed. Keep a reliable backup of the database directory – it is the key to your BIOCARD's – if you lose it you won't be able to erase/learn any of the existing BIOCARD's!

## Enrol Corporate User

**NOTE:** if you receive an error message stating '*the BIOCARD is locked and you do not have the correct key*' the database for the BIOCARD Manager application does not match serial number for the BIOCARD in use. Either locate the same database the BIOCARD was initialised with or return to the same computer/database the BIOACRD was initialised with. This is a security measure to ensure that only the original PC owner or administrator can enrol/erase their BIOCARDS.

To Enrol a corporate user to a BIOCARD:

1. Open the Microlatch BIOCARD Manager application.
2. Connect a BIOCARD to a USB port on your computer, using the USB Serial Programing cable that came with your Corporate Mode Starter Kit.
3. Click the 'Learn' button on the BIOCARD Manager application; A rotating Cyan light will appear around the BIOCARD button showing the device is waiting for a finger to be swiped.
4. Swipe a 'user' finger; the light indication will go blank for a second then start to rotate with Magenta light again. Repeat the finger swipe processes until you are presented with a solid green glow around the button (this takes up to approx. 10

swipes to get an accurate template of your fingerprint).

5. Repeat steps 3 and 4 until desire number of user fingers are enrolled.

## Erase Corporate User

NOTE: if you receive an error message stating '*the BIOCARD is locked and you do not have the correct key*' the database for the BIOCARD Manager application does not match serial number for the BIOCARD in use. Either locate the same database the BIOCARD was initialised with or return to the same computer/database the BIOACRD was initialised with. This is a security measure to ensure that only the owner can enrol/erase their BIOCARDS.

To erase all corporate users from a BIOCARD:

1. Open the Microlatch BIOCARD Manager application.
2. Connect a BIOCARD to a USB port on your computer, using the USB Serial Programming cable that came with your Corporate Mode Starter Kit.
3. Click the 'Erase' button on the BIOCARD Manager application; A solid Green light will flash around the BIOCARD button showing the device has been successfully erased.

# Chapter 5 - About the Battery

BIOCARD has an internal, non-replaceable battery. For best results, the first time you use the device, let it charge for about 3 hours or until the battery indicator shows the battery is fully charged.

## Battery indications:

- Red flash indicates low battery
- Blue fade indicates battery is being charged
- Green fade indicates battery fully charged



**NOTE** – The BIOCARD features a non-volatile memory. All fingerprint templates will remain securely in the device even when batteries are completely drained.

## Charging the Battery

You can charge the BIOACRD in two ways:

- Connect the BIOCARD to a USB port on your computer via the supplied USB Cable.
- Use a 5V USB Power Adaptor, available separately.

## Chapter 6 - Warranty Information

Microlatch Limited warrants this product to be free from defects in material and workmanship for a period of one (1) year from the date of purchase. The stamp of distributor and/or a copy of the original sales invoice are required as the proof of purchase for warranty repairs.

This warranty is limited at Microlatch's discretion to the replacement of any product proven to be faulty in manufacture or materials, with the same or equivalent product free of charge. Labour charges, transportation and other costs associated with the replacement or re-installation of the parts or products are excluded from this warranty and will not be paid by Microlatch. Please note these conditions in full within the relevant sales agreement at purchase.

Microlatch assumes no liability under the warranty for the following:

- Misuse, abuse, accidental or intentional damage
- Improper maintenance and installation
- Unauthorised repair or modification
- Use contrary to instructions from Microlatch
- Use of replacement parts other than authorized parts
- Deterioration in colour and performance of polymer materials

- Malfunction or failure of product due to the use of non-genuine, Microlatch parts.

To the extent permitted by law, Microlatch shall not be liable to the products, common user or any other person for any incidental or consequential damages arising howsoever and including but not limited to damages from and defects, malfunction, or failure of any product or component.

To the extent permitted by law, this warranty is the exclusive warranty granted by Microlatch and is in lieu of all other expressed or implied warranties.

There are no implied warranties as to merchantability, quality or fitness for a particular purpose, nor the security procedures employed or administered through issuance and thence for ongoing product / software management.

In all other respects the standard terms and conditions of Microlatch apply. This product is designed to form part of an access system, it requires a secured access reader in the same manner as any proximity card. This product cannot be used as the sole means for securing the access point.

Microlatch reserves the right to make changes to features and specifications at any time without notice and in the interest of product improvement.



***Microlatch***

Microlatch Limited

ABN 52 059 640 747

[www.microlatch.com](http://www.microlatch.com)

Microlatch™ and BIOCARD™ are registered

trademarks of Microlatch Pty Ltd

BIOCARD™ is a worldwide patented product.

PCT/2004/001083

© 2011 Microlatch™ All rights reserved

V0.1